THE INTERNATIONAL PRIVACY BULLETIN
PUBLISHED BY PRIVACY INTERNATIONAL

VOL 4 NO 2 SPRING 1996

IN SEARCH OF PERFECT IDENTITY

SIMON DAVIES

The accurate identification of individuals has always been a key concern for governments and private sector organizations. The development of identification systems is important to organizations because it offers one contributing solution to fraud and administrative inefficiency. Such initiatives can offer benefits to the client as well as to the administration. For these reasons, all organizations strive to achieve "perfect identity" of their clients.

Conventional forms of identification have always been subject to fraud and manipulation. Card systems are the most vulnerable. Fake "blanks" of even the highest integrity cards are generally available in Singapore or Thailand within weeks of issue.[1] The general availability of sophisticated computer machinery has placed the ability to forge such documents into the hands of a much wider group of criminals than would have been the case in earlier years.

One of the largest problems facing benefits organizations, however, is the existence of multiple identities. Since most card systems rely on a pre-existing numbering or registration system, problems in the pre-existing system will be compounded.

Many current number systems are inadequate. The Social Security Number (SSN) in the United States has become a defacto national identifier, despite admissions by the Social Security Administration that between four and ten million false or illegal numbers are in circulation. In Ontario, nearly twelve million Health Benefits Cards have been issued to a population of ten million. The government of Sweden, which instituted the first national number fifty years ago, is now claiming that the system facilitates fraud. Limitations are now being set on the uses of the number, and the Swedish Data Inspectorate is moving to break the number's "monopoly". Authorities in Australia have detected forged Tax File Numbers since their inception, and although internal studies and estimates have been made, the ATO refuses to divulge these figures.[2]

The development of high integrity identity systems is, however, fraught with problems. An overly rigorous identification procedure could prove unpopular, forcing some people to drop out of the system, and inviting a degree of civil disobedience in others. On the other hand, lax and ineffective procedures leave organizations vulnerable to fraud. A key focus of

Continued on page 14

PRIVACY INTERNATIONAL

Not Such a Good ID

ID card proposals currently being considered by the United States, Britain and Canada have sparked a range of concerns throughout the political spectrum.

This edition of the *IPB* discusses the many issues that are raised when ID cards are introduced into a democratic nation. The implications are profoundly important and very complex. At the heart of the ID card notion is a shift in the relationship between citizen and state, and an increase in a range of official powers. Any move in this direction should be made only after serious and genuine public consultation.

The purpose of ID cards varies from employment and welfare entitlement to law enforcement, but there is surprisingly little documented evidence to justify claims made about the need for the cards. Few police or criminologists have been able to advance any evidence whatever that the existence of a card would actually reduce the incidence of crime, or the success of prosecution. Their impact on illegal immigration has not been quantified, and claims made about the benefit of cards in the fight against tax evasion are generally unreliable.

More to the point are the hidden dangers that an official ID card brings with it. The entrenchment and expansion of criminal false identity is rarely addressed by authorities anxious to sell an ID card to the public. The implications of creating an internal passport are generally ignored, as is the growing body of evidence that ID cards foster an endemic component of discrimination.

Virtually all countries with ID cards report that their loss or damage causes immense problems. Up to five per cent of cards are lost, stolen or damaged each year, and the result can be denial of service ad benefits, and - in the broadest sense - loss of identity.

All ID cards - whether voluntary or compulsory - develop into an internal passport of sorts. Without care, the card becomes an icon. Its use is enforced through mindless regulation or policy, disregarding other means of identification, and in the process causing significant problems for those who are without the card. The card becomes more important than the individual.

Privacy International has opposed the introduction of these cards in many countries. We do so because the existence of a card challenges important precepts of individual rights and privacy. At a symbolic and a functional level, ID cards are an unnecessary and potentially dangerous white elephant. They are promoted by way of fear-mongering and false patriotism, and are implemented with scant regard for serious investigation of the consequences.

THE INTERNATIONAL PRIVACY BULLETIN
Published by Privacy International

VOL 4 NO 2 Spring 1996

CONTENTS

Republic became a member. Poland and Hungary joined in 1996. One of the central concerns of the OECD in Central Europe is to encourage the continued development of democratic institutions.

The OECD also has impressive hi-tech policy credentials. Distinguished international panels, led by well respected Australian jurist Michael Kirby, developed international policies for transborder data flows in 1980 and information security in 1992. The privacy policy became the basis for national law in more than a dozen European and Pacific rim countries. The information security guidelines were not easily translated into national law, but their influence is still recognized.

But when the OECD found itself looking for new projects after the information security study was completed, the US, a major funder of the organization then in arrears, had the answer: a new international policy for encryption. The topic was timely and renewed US interest in the OECD was welcome. The OECD had already begun a review of the issue. The OECD expert panel was quickly formed in Paris in December, 1995. A set of principles were drafted and discussed. Debate continued at a meeting in Canberra in February, 1996 and then in Washington, DC in May 1996. Further discussion is planned for late 1996. The outcome is still far from clear.

The OECD Comes to Washington

Many obstacles remain at the OECD for Clipper proponents. The OECD typically operates by a slow, consensus building process. Since the institution has no legal authority, and multiple political systems and cultural traditions must be brought together, every attempt is made to explore and analyze. National sovereignty is a sensitive issue.

Central to understanding the role of the OECD also is its commitment to democratic institutions. Indeed, to read the 1980 privacy principles is to be reminded once again that in democratic nations citizens have rights which governments must respect. Even the security policy, hardly the stuff of civics class, echoes the OECD's commitment. "The security of information systems should be compatible with the legitimate use and flow of data and information in a free society," states the Democracy Principle.

At its best, OECD policy-making can be an exhilarating process. Countries strive to find the common ground that will promote economic growth and respect national differences all the while recognizing that political liberty is an essential precondition for international policy. It is conceivable that such a process could be made to work for some of the hard problems facing the growing Internet community — intellectual property, content regulation.

IT IS AN EXTRAORDINARY SCENE, AS IF US TRADE OFFICIALS AND COMMERCE DEPARTMENT EXPERTS HAD BEEN MUGGED IN THEIR HOTEL ROOMS AND REPLACED BY AGENTS OF A DIFFERENT GOVERNMENT.

But the encryption policy has been unlike previous OECD efforts. The slow, deliberate consensus building effort that produced good polices on security and privacy has been pushed aside in favor of a fast-track strategy recommended by Washington. Government agencies responsible for trade and economic development were asked to step aside for law enforcement officials. The delegation from the United States to the economic organization is chaired not by a member of the Department of Commerce but by the head of the Justice Department's Computer Crime Unit. The NSA rep is close at hand. The former NSA general counsel records the minutes of the meetings for the benefit of his business clients and the US delegation. It is an extraordinary scene, as if trade officials and Commerce Department experts had been mugged in their hotel rooms and replaced by agents of a different government. The DOJ has even managed to place one of its own at the OECD to assist the organization in writing the guidelines in the shortened time-frame.

While early attempts by the US to spin off a secret drafting party ultimately failed, the US delegation — that is to say representatives of the Department of Justice and the National Security Agency and a few business representatives who stand to gain big if key escrow is adopted — succeeded in clouding two critical

sessions around the globe.

Whither Washington?

It is always hard to predict where the OECD countries will come down, but a quick survey suggests that key escrow has a long road ahead. The new government of Australia came into power in clear opposition to escrow encryption. Canada has always placed a premium on international human rights. Denmark's IT panel rejected key escrow. Germany must assess whether the key escrow plan favored by law enforcement outweighs the lost commercial opportunity of robust crypto exports. The Netherlands' delegate has spoken in opposition to the plan. New Zealand is likely to follow Australia's lead. Sweden is holding ranks with its Scandinavian neighbors. Turkey must decide if it will acede to technologies that will do little to promote economic growth. Even France, which clearly wants to maintain domestic surveillance capabilities, must consider if key sharing with foreign intelligence agencies is in its national interests.

Countries are well aware that encryption will pose new challenges to law enforcement. But it is becoming equally clear, as the US National Research Council concluded in a report earlier this year, that one of the best ways to prevent on-line crime and to protect public safety will be to promote the availability of strong encryption.

Indeed, the Japanese position, like the position of many OECD members, is not hard to understand. For the member nations of the OECD, encryption policy is first and foremost about the development of the technical infrastructure for secure on-line transactions to promote economic growth. To the extent that law enforcement concerns enter into the picture, they must be balanced by competing economic and civil liberty interests.

Washington Comes Home

Central to the current OECD debate about encryption policy is the interplay of two principles. The first — Free Choice — states that users and businesses should be free to use whatever form of encryption they wish without government restriction. The second — Government Access — has been described as establishing a government right to access encoded communication.

How are these principles to be reconciled? One approach would be to allow "free choice" within the narrow set of key escrow options. Such an approach is favored by some law enforcement officials but seems unlikely to sway most OECD members or US business.

The better answer for the OECD would be to leave the Free Choice principle in place as the cornerstone of international crypto policy and to treat Government Access principle not as a right to intercept but as an obligation for governments to comply with lawful process when interception occurs without imposing draconian key escrow systems. Such an approach would strengthen the hand of independent judiciaries, promote government accountability, and reaffirm the principle of private communication set out in the Universal Declaration of Human Rights.

AS THE US NATIONAL RESEARCH COUNCIL CONCLUDED IN A REPORT EARLIER THIS YEAR, THAT ONE OF THE BEST WAYS TO PREVENT ON-LINE CRIME AND TO PROTECT PUBLIC SAFETY WILL BE TO PROMOTE THE AVAILABILITY OF STRONG ENCRYPTION.

For governments in Eastern Europe and others struggling to build democratic institutions, it would also send a clear message that principles of liberty must place constraints on the government before the governed. And, consistent with the mission of the OECD, it would replace wartime policies with those intended to promote economic growth and international cooperation.

The traditions of the OECD weigh in favor of such an outcome. Indeed, the traditions of the United States would argue for this result as well.

Marc Rotenberg is director of the Electronic Privacy Information Center (http://www.epic.org). He served on the OECD expert panel on information security and currently advises the OECD Secretariat on encryption policy.

fraud. In evidence to the parliamentary committee investigating the proposal, the Department said that much less than one percent of benefit overpayments resulted from false identity. The Department decided that it would pursue other means of tackling fraud. The DSS in the UK argued against ID cards on the same grounds.

The Australian DSS estimates that benefit overpayment by way of false identity accounts for 0.6 per cent of overpayments, whereas non-reporting of income variation accounts for 61 per cent. The key area of interest, from the perspective of benefit agencies, lies in creating a single numbering system which would be used as a basis for employment eligibility, and which would reduce the size of the black market economy.

3. They Will Not Stop Illegal Immigration

The immigration issue appears to be the principal motivation behind ID card proposals in continental Europe, the United States and many developing nations.

The abolition of internal borders has become a primary concern of the new European Union. The development of the Schengen agreement between the Benelux countries, France and Germany calls for the dismantling of all border checks, in return for a strengthening of internal procedures for vetting of the population. France and the Netherlands have already passed legislation allowing for identity checks on a much broader basis, and other countries are likely to follow.

The establishment of personal identity in the new borderless Europe is a contentious issue, but is one which appears (to many people) to be a broadly acceptable trade-off for the convenience of total freedom of movement within the union.

The use of a card for purposes of checking resident status depends on the police and other officials being given very broad powers to check identity. More important from the perspective of civil rights, its success will depend on the exercise of one of two processes: either a vastly increased level of constant checking of the entire population, or, a discriminatory checking procedure which will target minorities.

The two arguments most often put forward to justify the quest to catch illegal immigrants in any country are (1) that these people are taking jobs that should belong to citizens and permanent residents, and (2) that these people are often illegally collecting unemployment and other government benefits.

The image of the illegal immigrant living off the welfare of the State is a powerful one, and it is used to maximum effect by proponents of ID cards. When the evidence is weighed scientifically, it does not bear any resemblance to the claim. When the Joint

THERE IS A POWERFUL RETRIBUTIVE THREAD RUNNING ALONG THE LAW AND ORDER ARGUMENT. SOME PEOPLE ARE FRUSTRATED BY WHAT THEY SEE AS THE FAILURE OF THE JUSTICE SYSTEM TO DEAL WITH OFFENDERS, AND THE ID CARD IS SEEN, AT THE VERY LEAST, AS HAVING AN IRRITANT VALUE.

Parliamentary Committee on the Australia Card considered the issue, it found that the real extent of illegal immigrants collecting government benefits was extremely low. The report described a mass data matching episode to determine the exact number. Of more than 57,000 overstayers in New South Wales, only 22 were found in the match against Social Security files to be receiving government unemployment benefits. That is, 22 out of a state population of five million. The Department of Immigration and Ethnic Affairs (DIEA) had earlier claimed that the figure was thirty times this amount (12.4 per cent as opposed to 0.4 per cent of overstayers).

Once again, immigration authorities worldwide base their estimates on qualitative assessment or, to put it more bluntly, guesswork. Again quoting from the Australia Card inquiry, "It became clear that the estimates for illegal immigrants were based on guesswork, the percentage of illegal immigrants who worked was based on guesswork, the percentage of visitors who worked illegally came from a Departmental report that was based on guesswork....The Committee

demand the production of national registration identity cards whenever they stop or interrogate a motorist for any cause....This Act was passed for security purposes and not for the purposes for which, apparently it is now sought to be used.... in this country we have always prided ourselves on the good feeling that exists between the police and the public, and such action tends to make the public resentful of the acts of police and inclines them to obstruct them rather than assist them.

6. They Tend to Become an Internal Passport

Virtually all ID cards worldwide develop a broader usage over time, than was originally envisioned for them. This development of new and unintended purposes has become known as function creep.

All compulsory ID cards - and even the majority of non-compulsory ones - develop into an internal passport of sorts. Without care, the card becomes an icon. Its use is enforced through mindless regulation or policy, disregarding other means of identification, and in the process causing significant problems for those who are without the card. The card becomes more important than the individual.

In most countries with a card, its use has become universal. All government benefits, dealings with financial institutions, securing employment or rental accommodation, renting cars or equipment and obtaining documents requires the card. It is also used in myriad small ways, such as entry to official buildings (where security will invariably confiscate and hold the card).

Ironically, many card subjects come to interpret this state of affairs in a contra view (the card helps streamline my dealings with authority, rather than the card is my licence to deal with authorities). The Australia Card campaign referred to the card as a licence to live.

7. A Voluntary Card Always Becomes Compulsory

Any official ID system will ultimately extend into more and more functions. Any claim that an official card is voluntary should not imply that a card will be any less of an internal passport than would a compulsory card. Indeed a voluntary card may suffer the shortcoming of limited protections in law. Comments by correspondents in many countries suggests that even where a card is voluntary it is so inconvenient not to have one that they are effectively compulsory.

During the campaign against the Australia Card, talk back radio hosts had become fond of quoting a paragraph of an HIC planning document on the Australia Card:

> It will be important to minimize any adverse public reaction to implementation of the system. One possibility would be to use a staged approach for implementation, whereby only less sensitive data are held in the system initially with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.

8. The Cost is Usually Extremely High

In the Philippines and Australia, the cost of implementing an ID system has been at the forefront of opposition. The Philippines proposal relied on government estimates that were drawn, as is often the case, from estimates calculated by computer industry consultants. These were found to under-estimate the true cost by eight billion pesos over seven years. The proposal lapsed because of this factor.

ALL COMPULSORY ID CARDS - AND EVEN THE MAJORITY OF NON-COMPULSORY ONES - DEVELOP INTO AN INTERNAL PASSPORT OF SORTS.

In Australia, the cost of the proposed ID card failed to take into account such factors as training costs, administrative supervision, staff turnover, holiday and sick leave, compliance costs, and overseas issue of cards. Other costs that are seldom factored into the final figure (as was the case in Australia) are the cost of fraud, an underestimate of the cost of issuing and maintaining cards, and the cost to the private sector.

systems, is not the inevitable conflict with civil rights. It is the curious repercussion that a card actually entrenches crime. By providing a one stop form of identity, criminals can easily use cards in several identities. Even the highest integrity bank cards are available as blanks in such countries as Singapore for several dollars. Within two months of the new Commonwealth Bank high security hologram cards being issued in Australia, near perfect forgeries were already in circulation.

This argument has been advanced in Australia, the UK, and the Netherlands. It relies on the simple logic that the higher an ID card's value, the more it will be used. The more an ID card is used, the greater the value placed on it, and consequently, the higher is its value to criminal elements. Organizations come to rely on the card as an unquestioned proof of ID, and often abandon the checking systems that have evolved over many years.

12. They Compromise National Identity and Personal Integrity

ID cards strike a nerve in the national psyche of some countries. ID cards are often viewed as inimical to the struggle for independence, freedom, autonomy and individuality that nations cherish. The Australia Card campaign vividly illustrates this phenomenon.

Privacy protection involves resistance to the establishment or consolidation of monolithic information systems. Informational chaos among agencies has ensured that the individual has not become a servant to the state. Variety, choice, and chaos have also had the effect of ensuring the free movement, rights, and free choice of individuals.

The movements against ID cards in the US, Canada, Australia, and New Zealand have highlighted a number of abstract fears, widely held throughout the population, such as:

- people will be de-humanised by being reduced to numbers;
- the system is a hostile symbol of authority;
- society is becoming driven by technology driven bureaucracy, rather than by elected government;
- such identification schemes are the mechanism foretold in religious prophecy (e.g. 'the Mark of the Beast').

While these fears may be dismissed by proponents of ID card, they ultimately will be the fuel for public disquiet.

Conclusion

Generally speaking, the key element of any modern ID card is the number. The number is the common element within all databases, and is the key to access all this personal information. With this number, governments can establish computer linking programs that merge information on many aspects of a person's life.

Privacy International has set up an extensive web page on national ID cards including a 7,000 word Frequently Asked Questions (FAQ) report, a summary of views from around the world, an analysis of successful campaigns, and other materials or current proposals in the UK and from around the world. The web page address is: http://www.privacy.org/pi/activities/idcard/

of the US is in the final stages of developing a biometric fingerprinting system using neural networks. Laboratory tests commissioned by the manufacturer are showing an accuracy of 99.99 percent, and a false rejection rate (rejecting genuine clients) of 0.1 percent Known as Printscan 3, the device is expected to cost US$600 per unit.[7]

The Japanese Telecommunications giant NTT recently announced the development of a fingerprint recognition method that appears to be exceptionally fast and accurate. The technique can be used in conjunction with ordinary information processing and communications systems. Recognition of a fingerprint takes place in an average of two seconds on a personal computer or one second on a workstation, with accuracy above 99.9 percent. Along with many other diverse applications, it can be used to confirm that the bearer of a credit card or ID card is the rightful owner. National computerised fingerprint systems are now being developed in several countries. The first national system was developed in Australia in 1987 using Fujitsu technology.[8]

The development of hand geometry, involving a scan of the shape and characteristics of the entire hand, has been an alternative approach in situations where there is public sensitivity to fingerprinting. Hand geometry is already employed in over 4,000 locations in the US and Europe, including airports, day care centers, nuclear research establishments, computer facilities, sperm banks, hospitals and in high security government buildings. [9]

An automated immigration system developed by the United States Immigration and Naturalization Service (INS) uses hand geometry (see below). In this project, frequent travellers to the United States have their hand geometry stored in a "smart" computer chip card. The traveller places a hand onto a scanner, and places the card into a slot. However, a similar project which was to commence shortly in Germany apparently rejected the hand geometry system because of inaccuracies in the technology. The problem demonstrates the extent to which controlled laboratory trials are of limited value in the real world.[12]

This system has the potential to pioneer a worldwide biometric system. It is feasible that within fifteen years, all countries will introduce such systems, and share this information. Some experts believe that by 2010, all travellers to and from the United States will need to be biometrically registered. Information about passengers will be shared on the basis of the biometry.

Countries around the world are jumping on the bandwagon. Spain is planning a national fingerprint system for unemployment benefit and healthcare entitlement. Russia has announced plans for a national electronic fingerprint system for banks. In the near future, Jamaicans will need to scan their thumbs into a database before qualifying to vote at elections. In the US, Blue Cross and Blue Shield have plans to introduce nationwide fingerprinting for hospital patients. This may be extended into more general medical applications. In Europe, tests are under way with equipment that puts a person's fingerprint information onto his or her credit card so a device at the point of purchase can compare the card's data to a fingerprint to assure that the use of the card is legitimate. In Australia, the technology is being used in retail outlets, government agencies, prisons, police forces and automated-teller machines. As it becomes more viable, biometric technology is likely to be adopted as the identification of choice for large, complex organizations.

"WITH THIS TECHNOLOGY, THE GOVERNMENT CAN COMPILE A DOSSIER ON A PERSON THAT TRACKS HIS EVERY PURCHASE AND MOVEMENT. THAT SORT OF THING IS POSSIBLE NOW, BUT IT IS TOO LABOR-INTENSIVE AND EXPENSIVE."

DANIEL POLSBY
NORTHWESTERN UNIVERSITY

Giving Welfare a Hand in the UK

In January 1994, senior officials of the UK Department of Social Security met with their chief, Peter Lilley to discuss ways of reducing welfare fraud,

for Travellers), the lane identifies passengers from the characteristics of their hand, rather than from their passport and photograph. It then connects with the standard immigration computer systems to determine the passenger's status.

These automated immigration lanes are appearing throughout the world - in Toronto, Frankfurt, Amsterdam, and on the US-Mexico border - as part of an international experiment intended to revolutionize the world's immigration systems.

The project, called INSPASS (Immigration and Neutralization Service Passenger Accelerated Service System), has for the past fourteen months been operating as a voluntary system for frequent travellers. More than 65,000 people have so far enrolled in the system, a figure which increases by almost 1,000 a week. Governments in 26 countries - including the UK - are coordinating with the project.

If the INSPASS trial is successful, the technology may ultimately make conventional ID cards and passports redundant. And, as a trade-off for faster immigration processing, passengers will have to accept a system which has the potential to generate a vast amount of international traffic in their personal data. Ultimately, a universal immigration control system may be linked to a limitless spectrum of information, such as police and tax systems.

An in-house evaluation of the system has given INSPASS the green light. INS officials are now confident that a universal project can be established, using common international standards and a smart card system that can cope with either a hand geometry or a fingerprint scan. According to staff working with the INSPASS project, all European governments are committed to the goal of automated immigration processing.

The thorny question is whether such a system might ultimately be manipulated by governments and airline companies anxious to receive more information about passengers.

Future Imperfect ?

To date only limited testing of biometrics has been carried out by independent agencies. Best known

How INSPASS Works

INSPASS is available to frequent travellers to and from the US, who are US or Canadian Nationals, or Nationals of the 32 countries involved in the US visa waiver scheme. The countries participating in the trial are Andorra, Austria, Belgium, Bermuda, Canada, Denmark, Finland, France, Germany, Iceland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, The Netherlands, New Zealand, Norway, San Marino, Spain, Sweden, Switzerland and the United Kingdom. Travellers who visit the United States at least three times a year are "invited" to apply in writing for INSPASS registration. Applicants then attend one of the INSPASS enrollment centres at JFK or Newark airports, where they are interviewed, and their identity confirmed.

This completed, the traveller places the palm of a hand onto the surface of a scanner, which then records intricate measurements and details of the hand's shape and contours. These are converted into a "template" and stored on a card (currently a paper card, but soon to be a smart card). Fingerprints are also taken and recorded at this point.

Whenever INSPASS members enter the two test airports, they bypass the main immigration queues, and go straight to the INSPASS "Kiosk". Once inside, the card is presented to the terminal, which confirms its' status. The hand is then placed onto a scanner. This matches the biometry of the palm with the "template" encoded into the card. The Immigration Information systems are consulted. Once the last of five green lights appear at the tips of the fingers, the glass exit door opens, and the passenger continues to the baggage claim and customs zone.

An increasing number of countries are already subscribing to a "Blue Lane" information exchange system in which passenger information is transmitted in advance of the journey.

social, legal, and political issues. Modern identification systems rely on technology that is far from proven. Biometric systems have not been tested on a nationwide basis. They are, to a different and perhaps lesser extent, subject to the same problems that exist at present in more conventional ID schemes.

The administrative and IT systems that form the basis of such ID schemes have been shown in several countries to be much less accurate and cost effective than was originally estimated. Years after the governments of the United States and Australia developed schemes to match public sector computers to save money, there is still no clear evidence that the strategy has succeeded in achieving its original goal. The audit agencies of both federal governments have cast doubt that computer matching schemes deliver savings in many key areas.

There are a great many complexities involved in the introduction of modern identity systems. The integration of computer systems and the merging of information brings with it the need for major organizational restructure. The use of identity procedures also changes the nature of relationships and transactions between clients and departments. Flawed technology has caused grief for organizations that rely on a consistent relationship with their client base. History shows that many organizations are not prepared to take these factors into account.

Any discussion of the risks involved in an integrated ID scheme will intersect considerably with concerns over computerization in general. The vulnerabilities of a computerised biometric system - at a human and organizational level - are very similar to the vulnerabilities of any integrated information system. All modern nationwide ID schemes are part of a larger information strategy. ID cards or biometric templates are used for several purposes, and are the basis of the sharing of data among organizations.

Problems of privacy and confidentiality are perhaps the most important non-budgetary problems created by these proposals. On the one hand, computers offer the promise of creating secure communications through encryption of information. On the other hand, they tend to be a conduit for the distribution of information to a great many locations, and they thus increase the risk of unauthorized access and unforseen use. Systems designers are often fixated by the theme of security, without glancing at the larger picture of how data is collected and distributed.

There exists a number of obvious privacy problems with any system that entails the establishment of a central registry, or even a distributed, but interconnected repository of personal identities. It is uncertain whether the establishment of a repository of identification data would be covered by many data protection laws. A biometric print may be considered in the public domain, or it may find its way into general use by way of implied consent of the individual. In this way, people may find that they are required to provide a biometric print in many unforseen or unintended future circumstances.

Identification systems throughout the world have a history of being ultimately used for unintended purposes. The Social Security number in the US and the Tax File Number, the Dutch SOFI number, and the Austrian Social Security number have been extended progressively to include such facets as unemployment benefits, pensioner benefits, housing entitlement, bank account verification, and higher education. There is a very real possibility that anything as widespread as a general purpose biometric system could mutate. The mere existence of a multi-purpose system of this magnitude will create irresistible opportunities to collect vast amounts of personal information .

MODERN IDENTIFICATION SYSTEMS RELY ON TECHNOLOGY THAT IS FAR FROM PROVEN. BIOMETRIC SYSTEMS HAVE NOT BEEN TESTED ON A NATIONWIDE BASIS. THEY ARE, TO A DIFFERENT AND PERHAPS LESSER EXTENT, SUBJECT TO THE SAME PROBLEMS THAT EXIST AT PRESENT IN MORE CONVENTIONAL ID SCHEMES.

At a society-wide level, the creation of a biometric system involves a number of risks. Privacy advocates

PRIVATE PARTS

AN AD-HOC COLUMN OF MISCELLANEOUS ITEMS

Albania

The Albanian Supreme Court on April 23 rejected an appeal by 13 deputies who have been banned from running in the upcoming general elections, Albanian media reported. A commission screening candidates for the elections ruled that they have a communist past. The Supreme Court rejected the deputies' request that they be given access to the documents on which the commission based its decision. It argued that there was enough evidence against them, since their names were included in a file listing those who collaborated with the Sigurimi, the communist-era secret service. Another 26 deputies have also appealed to the court. (Fabian Schmidt, OMRI Inc., April 24, 1996).

Australia

The New South Wales Attorney General announced new privacy legislation on April 4. The Privacy Committee would be merged with the Discrimination board and would be given subpoena powers. Individuals that had their personal information abused by government officials could be compensated up to $40,000 and criminal changes could be brought against the official. The legislation was advanced after it was revealed that a Department of Community Services official had stolen the file of a state ward. (*Australian Associated Press*, April 4, 1996).

Austria

The Austrian government rejected attempts by the European Union to pressure it to change current laws which allow for anonymous bank accounts. The EU claims that the law violates the EU directive on money laundering. Viktor Klima, the finance minister, said Austria was prepared to defend its case at the European Court. Austria is the only country in the EU that allows for anonymous accounts. There are an estimated 26 million accounts. (*Financial Times*, April 10, 1996).

Canada

Ontario Health Minister Jim Wilson announced on Feb. 12 the creation of a combined health card, driver's licence, senior's card and welfare identification card. The new card may use a thumb print electronically scanned into the system. It is expected to be used by all ministries and will cost an estimated $1 billion. (*The Ottawa Citizen*, February 13, 1996).

European Union

American and European direct marketers are lobbying the EU to drop its plans to enact a directive on the privacy of personal information on telecommunications networks. The marketers are urging that the EU allow them to police themselves. (Direct Marketing News Online, May 6, 1996).

Finland

Finnish bank Merita and online merchants have launched a digital cash service using an anonymous digital cash system designed by Amsterdam-based Digicash Inc. Merchants include Internet provider EUnet, the Finnish Securities and Derivatives Exchange and several newspapers, television companies, and online shopping companies. (*Reuters*, March 12, 1996).

France

The National Commission for the Control of Security Interceptions said in its annual report on March 28 that an estimated 100,000 illegal wiretaps were conducted every year in France, mainly by government agencies. It also reported that 15,000 taps are legally authorized each year. (*Reuters*, March 28, 1996).

The Council of Europe ordered France to pay

ADVANCED SURVEILLANCE TECHNOLOGIES CONFERENCE II

Sponsored by

Privacy International
Electronic Privacy Information Center

September 16, 1996

Citadel Ottawa Hotel and Convention Centre
Ottawa, Canada

The rapid evolution of technology is leading to the creation of a seamless web of surveillance across much of the world. Powerful technologies originally developed for the military are being adopted by law enforcement and civilian agencies, and private companies to monitor entire populations. This has been further fueled by the end of the Cold War and increasing demands for greater bureaucratic efficiency. Existing laws and regulations have failed to keep up with these developments.

This one day conference will examine a range of advanced surveillance technologies and their impact on privacy and other civil liberties. It will explore the process of planning and implementation of the technologies, their operating conditions, and the people and organizations responsible for them. The conference will also examine possible technical, regulatory, and legal responses.

The conference will also address in detail the findings of Privacy International's "Big Brother Incorporated" report which examined the international trade in surveillance technology and the involvement of the arms industry.

LIST OF SPEAKERS AND TOPICS

An Introduction to New Surveillance Technologies
- Dave Banisar, Electronic Privacy Information Center & editor, *International Privacy Bulletin*

Tracking the Surveillance Trade
- Simon Davies, London School of Economics & Director, Privacy International

Surveillance Technologies of the Intelligence Agencies
- Mike Frost, former intelligence officer, Canadian Communications Security Establishment & author, *Spyworld*

SIGINT Online: Signals Intelligence on the Net
- Wayne Madsen, author, *Handbook of Personal Data Protection*

Datamining the Net: Cookies, Crawlers and Trackers
- Simson L. Garfinkel, author, *Practical Unix and Internet Security*

Intelligent Vehicles and Tracking
- Phil Agre, University of California, San Diego

Its all in the Genes: The Human Genome Project and Privacy
- Pierrot Peladeau, Progesta Inc. & editor *Privacy Files*

A Privacy Commissioner Case Study: Introduction of a DNA Profile Databank to New Zealand
- Bruce Slane. New Zealand Privacy Commissioner

The Role of Law in Protecting Privacy: A Comparative Overview
- Colin Bennett, University of Victoria

COSTS

US$175 for Commerical Organizations/Government Agencies
US$75 for Individuals/Non-profit Organizations

More information on the conference is available at the PI Home Page at http://www.privacy.org/pi/conference/ottawa/or contact pi@privacy.org. A mailing list for future information is available at pi-news@privacy.org (subject: subscribe).